UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/555,408	11/01/2005	Ahmed El-Sayed Ahmed	2847-72452-01	9403

24197   7590   11/08/2010
KLARQUIST SPARKMAN, LLP
121 SW SALMON STREET
SUITE 1600
PORTLAND, OR 97204

EXAMINER
KANAAN, SIMON P

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
11/08/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

tanya.harding@klarquist.com
docketing@klarquist.com

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 August 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-12,14 and 19-31* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-12,14 and 19-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This office action is in response to applicant's amendment filed on 9/26/2010 for

Application No. 10/555408.

2.   Applicant's arguments/ amendments with respect to pending claims 1-5, 7-12, 14, and

19-31 filed 9/26/2010, have been fully considered but are moot in view of new grounds of

rejection necessitated by the amendments.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

4.   Claims 1-2, 4-5, 7-12, 19-26 are rejected under 35 U.S.C. 103(a) as being unpatentable

by Brown et al. (U S Patent Number 5,557,686) in view of Dov Jacobson (US Pre-Grant

Publication No: 2005/0008148) hereinafter referred to as Jacobson..

        As per claims 1, 25 and 26, Brown discloses: a behavioral biometrics based user

verification system for use with an input device, said system comprising a data interception unit

configured to intercept inputs from a user that are directed to an application - Brown, column 2

lines 15-19, collecting samples containing typing characteristics of an authorized user based on

key press times and key release times is a behavioral biometrics based system which intercepts

data from a user, data is collected and then user is asked to enter data, an application is running

which asks the user for input hence the data is directed towards an application,

a behavior analysis unit operatively coupled to said data interception unit - Brown,

column 2, lines 20-22, vectors constructed for purifying the samples are behavioral analysis units

since they contain behavioral data,

and a behavior comparison unit operatively coupled to said interception unit, wherein

said system translates behavioral biometrics information into representative data. - Brown,

column 2, lines 28-29, the neural network trained to output whether an input is from an

authorized user is representative data of biometric information,

stores and compares different results, and outputs a user identity result associated with

user authorization of the user. - Brown, column 2, lines 30-32 and 38-38, the user typing the

previously determined keystroke sequence into the neural network then having the neural

network determine whether the user is authorized, is storing and comparing the different results

and outputting the user identity result.

But fails to disclose the input device is a mouse, and data interception is directed towards

an application other than a user authentication application and wherein the data interception unit

is configured to passively collect at least one mouse movement data, mouse point and click data,

and mouse drag and drop data generated in response to usage of the mouse in providing input to

the application other than the user authentication application;

However, Jacobson discloses the input device is a mouse, - Jacobson, figure 1, teaches

data input device being a mouse

and data interception is directed towards an application other than a user authentication application and wherein the data interception unit is configured to passively collect at least one mouse movement data, mouse point and click data, and mouse drag and drop data generated in response to usage of the mouse in providing input to the application other than the user authentication application; - Jacobson, [0072] and [0075], teaches monitoring mouse movement data for applications other than authentication application such as signing up for a credit card, i.e. it passively collects mouse data for applications other than the authentication application and [0054] teaches mouse data includes speed, acceleration, drag, click duration, double click rhythm etc..

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the passively collecting mouse movement data method of Jacobson with the behavioral biometric based system of Brown because having a continuous authentication method makes theft more difficult and less likely since it continuously checks up on registered user.

As per claim 2, Brown in view of Jacobson discloses the user verification system of claim 1, wherein said system is suitably configured for real-time monitoring - Brown, column 13 lines 52-55, system notifying a system operator that user has not passed keystroke is real-time monitoring

As per claim 5, Brown in view of Jacobson discloses the limitations of claim 4, wherein said data interception unit is further configured to characterize movement based on at least one

of average speed, average traveled distance, and direction of movement. - Jacobson, [0054]

teaches mouse data includes speed, acceleration, drag, click duration, double click rhythm etc.

As per claim 7, Brown in view of Jacobson discloses the limitations of claim 1, wherein

said data interception unit is further configured to identify action from a mouse as one of drag

and drop, point and click, mouse movement, and silence, such that in use, said system receives

data from a mouse - Jacobson, [0054] teaches mouse data includes speed, acceleration, drag,

click duration, double click rhythm etc.

As per claim 8, Brown in view of Jacobson discloses the limitations of claim 1 but fails to

disclose expressly the limitation in claim 7, wherein said data interception unit is further

configured to characterize movement based on at least one of average speed, average traveled

distance, and direction of movement. - Jacobson, [0054] teaches mouse data includes speed,

acceleration, drag, click duration, double click rhythm etc.

As per claims 20, Brown in view of Jacobson discloses the system of claim 1, wherein

the behavior comparison unit is configured to produce the user identity result based on mouse

movement speed compared to traveled distance, average speed per direction of movement, a

distribution of movement directions, average speed with respect to action type, a distribution of

actions, a distribution of traveled distance, and a distribution of movement elapsed time. -

Jacobson, [0054] teaches mouse data includes speed, acceleration, drag, click duration, double

click rhythm etc.

As per claim 24, Brown in view of Jacobson discloses the system of claim 1, wherein the behavior analysis unit is configured to establish a user signature based on a plurality of sessions in an enrollment mode. –Brown, column 2, lines 12-25, multiple user samples are used in authentication process.

As per claim 9, Brown discloses: A method of characterizing a user comprising the steps of: receiving data associated at a user application; passively intercepting at least a portion of the received data and forwarding the intercepted data to a behavioral processing unit; processing the intercepted portion so as to develop a signature for a user. - Brown, column 2 lines 15-19, a keyboard is a motion-based input device which is used to collect data, an application is running which asks the user for input hence the data is directed towards an application, AND Brown column 2 lines 20-22, vectors constructed for purifying the samples are behavioral analysis units since they contain behavioral data and column 2 lines 28-29, the neural network trained to output whether an input is from an authorized user is representative data of biometric information, AND Brown column 2 lines 30-32 and 38-38, the user typing the previously determined keystroke sequence into the neural network then having the neural network determine whether the user is authorized is a model of users signature.

But fails to disclose the input device is a mouse, and data interception is directed towards an application other than a user authentication application and wherein the data interception unit is configured to passively collect at least one mouse movement data, mouse point and click data,

and mouse drag and drop data generated in response to usage of the mouse in providing input to the application other than the user authentication application;

However, Jacobson discloses the input device is a mouse, - Jacobson, figure 1, teaches data input device being a mouse

and data interception is directed towards an application other than a user authentication application and wherein the data interception unit is configured to passively collect at least one mouse movement data, mouse point and click data, and mouse drag and drop data generated in response to usage of the mouse in providing input to the application other than the user authentication application; - Jacobson, [0072] and [0075], teaches monitoring mouse movement data for applications other than authentication application such as signing up for a credit card, i.e. it passively collects mouse data for applications other than the authentication application and [0054] teaches mouse data includes speed, acceleration, drag, click duration, double click rhythm etc.

As per claim 4 and 22, Brown in view of Jacobson discloses the system of claim 1, wherein the limitations of claim 1 and 9 respectively, wherein said data interception unit is configured to identify data based on mouse movement between first and second locations, wherein movement between the first and second locations is not associated with a mouse click - Jacobson, [0054] teaches mouse data includes speed which is movement from one location to another not associated with a mouse click.

As per claim 10, Brown in view of Jacobson discloses the system of claim 1, wherein the method of claim 9, further comprising comparing said signature with a signature of an authorized user - Brown, column 2 lines 30-32 and 38-38, the user typing the previously determined keystroke sequence into the neural network then having the neural network determine whether the user is authorized is a model of users signature.

As per claim 11, Brown in view of Jacobson discloses the system of claim 1, wherein the method of claim 10, further comprising filtering said data after processing and before developing the signature to reduce noise - Brown, column 4 lines 30-35, purifying users input files is filtering the processed data before modeling and reduces noise.

As per claim 12, Brown in view of Jacobson discloses the system of claim 1, wherein the method of any one of claims 11, further comprising collecting and processing and developing the signature in real-time - Brown, column 14 lines 7-18, continuously updating the users profile with new samples is a method which collects, processes and models data in real-time, modeling the data is the user signature.

As per claims 14, Brown in view of Jacobson discloses the system of claim 1, wherein the limitations of claim 9, wherein said collecting data further comprises characterizing movement based on at least one of average speed, average traveled distance, and direction of movement - Jacobson, [0054] teaches mouse data includes speed, acceleration, drag, click duration, double click rhythm etc.

As per claim 19, Brown in view of Jacobson discloses the system of claim 1, wherein the behavior comparison unit is configured to store user identities for a plurality of potential users, and the user identity result identifies the user from among the plurality of potential users. – Brown, column 2, lines 16 and 17, plurality of users are authorized for system, i.e. authentication information is stored for multiple users of the system

As per claim 21 Brown in view of Jacobson discloses the method of claim 9, wherein the signature for the user is developed based on movement speed compared to traveled distance, average speed per direction of movement, distribution of movement directions, average speed with respect to action type, a distribution of actions, a distribution of traveled distance, and a distribution of movement elapsed time. - Jacobson, [0054] teaches mouse data includes speed, acceleration, drag, click duration, double click rhythm etc.

As per claim 23, Brown in view of Jacobson discloses the method of claim 9, wherein the behavioral biometric information from the mouse is obtained in a background process- Jacobson, [0072] and [0075], teaches monitoring mouse movement data for applications other than authentication application such as signing up for a credit card, i.e. it passively collects mouse data for applications other than the authentication application

As per claim 28, Brown in view of Jacobson discloses the method of claim 9, wherein the signature for the user is developed based on a distribution of traveled distances. - Brown, column

2 lines 20-22, vectors constructed for purifying the samples are behavioral analysis units since

they contain behavioral data and Jacobson, [0054] teaches mouse data includes speed,

acceleration, drag, click duration, double click rhythm etc..

5.   Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable by Brown in view of

Jacobson and further in view of Mizutome et al. (US Pre-Grant Publication No: 2002/0078447).

        As per claim 27, Brown in view of Jacobson discloses system of claim 1,

        But fails to disclose wherein the behavior comparison unit is configured to produce the

identity result based on a histogram of mouse movement directions.

        However Mizutome discloses wherein the behavior comparison unit is configured to

produce the identity result based on a histogram of data associated with input device.

        It would have been obvious at the time of the invention to modify the data collection

system used for authorizing a user in Brown with the data collection system of storing the data in

a histogram as taught by Mizutome because a histogram is a well known method for collecting

and displaying data.

6.   Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Brown in view of

Jacobson in further view of Boebert et al. (US Patent Number 5,596,718).

        As per claim 3, Brown in view of Jacobson discloses: the limitations of claim 2

        But fails to disclose further comprising secure communication protocols operatively

couple to said data interception unit.

Boebert discloses: further comprising secure communication protocols operatively couple

to said data interception unit; - Boebert, column 3 lines 26-29, an inserted trusted path between

input/output devices and work station is a secure communication protocol between the system

and data interception.

It would have been obvious to one of ordinary skill in the art at the time of the invention

to incorporate the secure communication between input device and system of Boebert with the

behavioral biometric based system of Brown because it would deter malicious hard ware or

software from emulating and listening to the communication path between the user and system -

Boebert, column 1 lines 30-35.

Conclusion

7.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571)270-3906. The examiner can normally be reached on Mon-Thurs 7:30-5:00 EST.

If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Gilberto Barron, can be reached at the following telephone number: (571) 272-3799.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/SIMON KANAAN/
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432